WARNING

～クラウドサービスやテレワーク環境を利用する際の個人情報の漏えいに関する注意喚起～

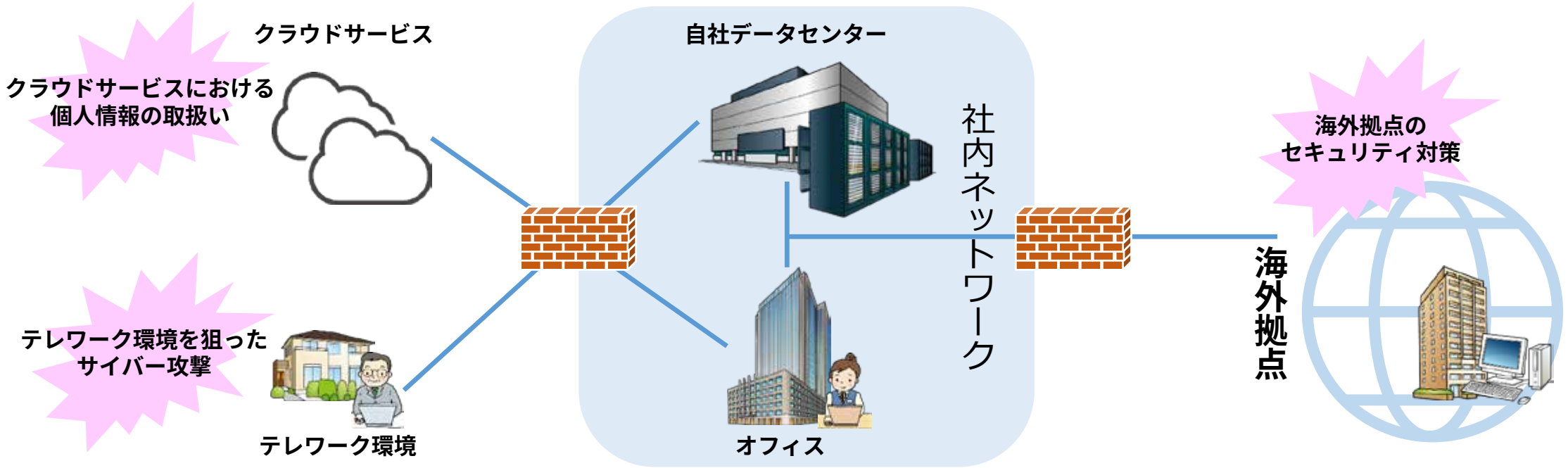
令和３年２月８日

個人情報保護委員会
Personal Information Protection Commission

はじめに

最近、従業員の様々な働き方に合わせてクラウドサービスやテレワーク環境などを導入する企業が増えています。一方、これらのシステム環境を狙ったサイバー攻撃も増加しており、個人情報保護委員会には、これらのシステム環境等において発生した個人情報の漏えい事案が多数報告されています。

今回は実際に発生した事例を紹介しますので、個人情報取扱事業者の皆様にはこちらをご参考の上、自組織が利用するシステム環境の見直しをお願いします。



発生事例から学ぶセキュリティ対策

　当委員会が報告を受けた個人情報の漏えい事案の中でも、今後も同様のケースが発生しうる事例について紹介します。
　自組織のセキュリティ対策が十分であるかチェックするために、システム担当者やシステム開発・保守運用の委託先等に対策の実施内容及び実施結果（証跡）を確認し、不十分であれば必要な対策を検討・実施しましょう。

＜事例＞

事例１　本来は非公開とすべきクラウドサービス上の個人情報を誤って公開してしまったケース

事例２　クラウドサービスへのログイン認証が十分でなく不正ログインを受けたケース

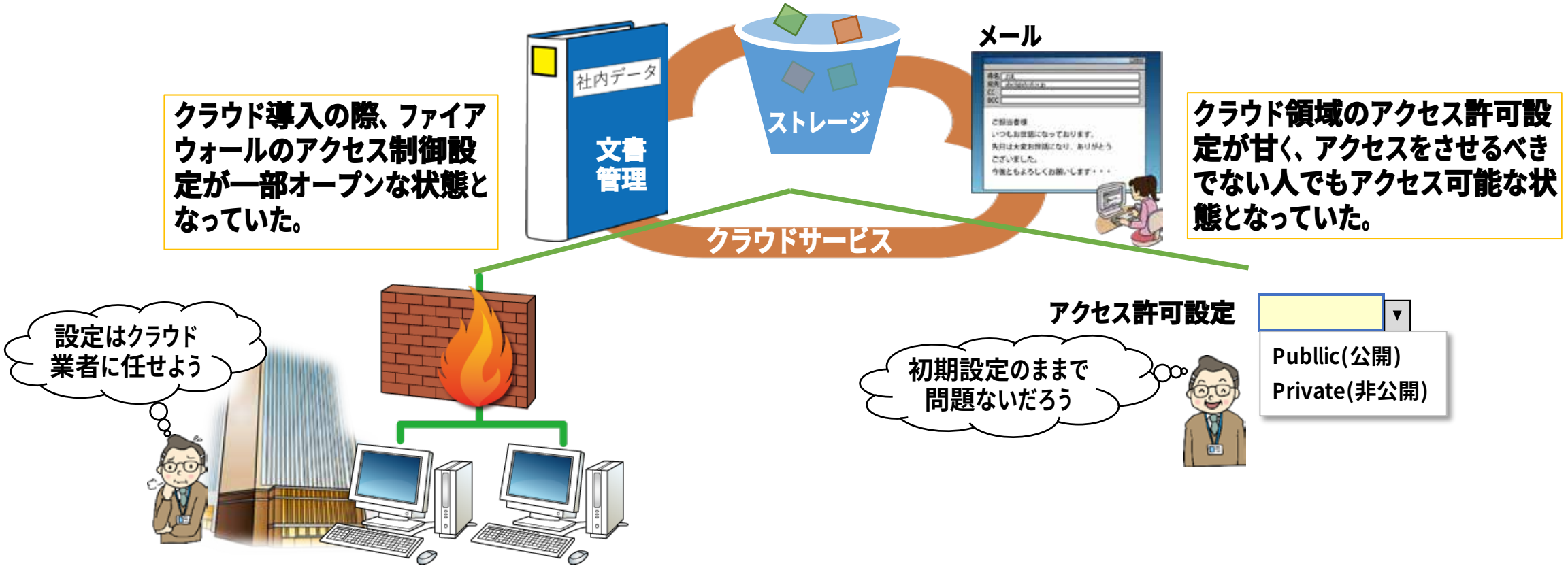
事例３　クラウドサービスのシステム管理者用の認証情報が適切に管理されていなかったケース

事例４　不正に入手したVPN認証情報を用いて個人情報を狙うサイバー攻撃

事例５　海外拠点経由のサイバー攻撃により国内ネットワークまで侵入されたケース

事例１　本来は非公開とすべきクラウドサービス上の個人情報を誤って公開してしまったケース

クラウドサービスの公開設定のミスにより、クラウドサービスに保存した個人情報を含む非公開情報が誰からでも閲覧可能な状態になってしまいました。原因は下図のようにファイアウォールの設定やデータ領域のアクセス許可の設定が正しく行えていなかったことが挙げられます。



次ページで
POINTと対策例を解説します。

事例１　本来は非公開とすべきクラウドサービス上の個人情報を誤って公開してしまったケース

＜陥りやすいPOINT＞

- ネットワークのセキュリティ設定はクラウド業者側で行われるものとの誤った認識があった。
- 利用するクラウドサービスによっては初期設定のままだと全ての人に公開する設定となっているが、それに気が付かなかった。

Ø **利用する事業者側で確認すべき事項についての知識・認識がなく、きちんと確認が行われなかったことによるもの。**

＜対策例＞

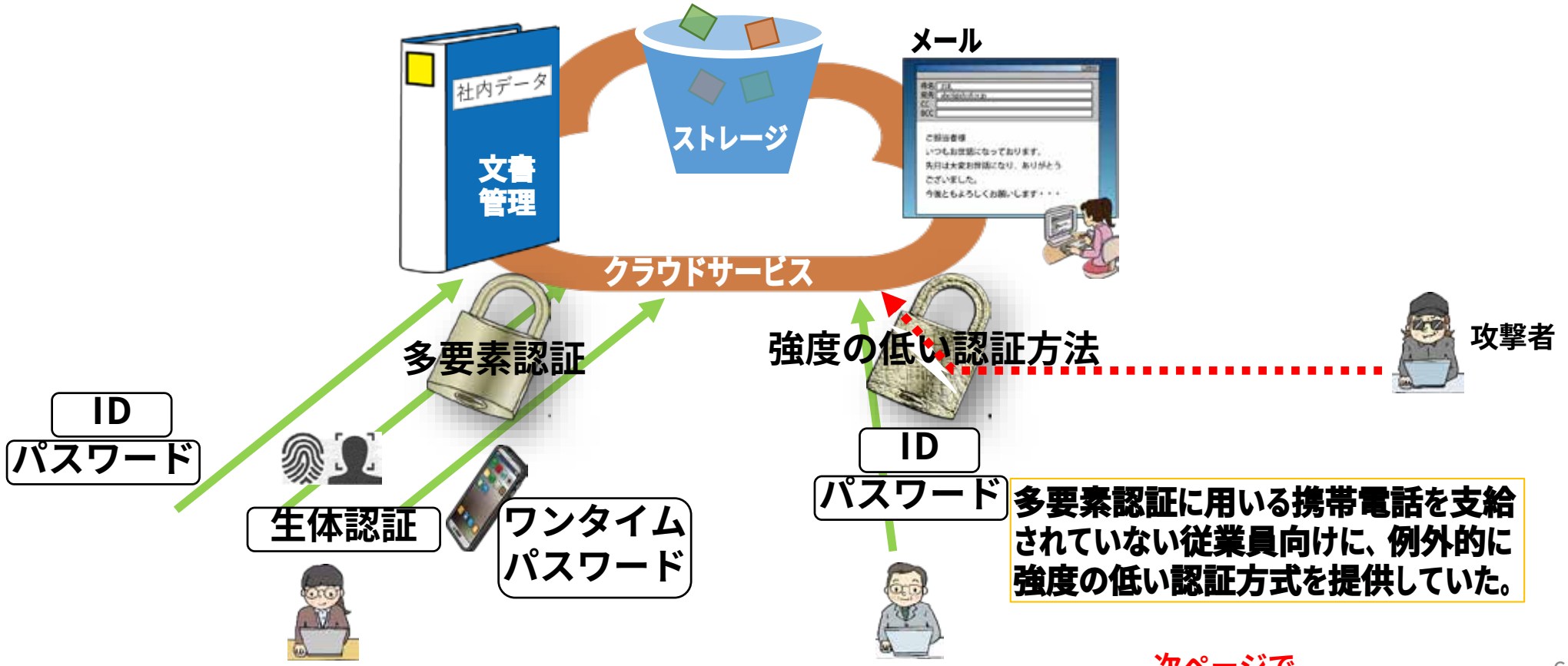
- 利用するクラウド毎の責任共有モデル(※)を確認し、クラウド業者の責任範囲と自社の責任範囲を正しく理解する。自社の責任範囲であるネットワーク設定（セキュリティグループ）、ストレージ公開設定、オブジェクト参照権限は適切であるか確認する（業務を委託している場合は委託業者に確認を徹底させる）。
- 初期設定も含めて現状の設定内容を確認し、設定変更する必要があるかどうか確認する。

※クラウド業者側と利用者側の双方で役割を分けて、全体のセキュリティを担保しようという考え方

Ø **クラウドサービスはインターネットを用いることでどこからでもアクセス可能であり便利ですが、その分セキュリティ対策は厳重に行う必要があります。対策が十分であるか不明な場合は、専門の事業者に相談することもご検討ください。**

事例２　クラウドサービスへのログイン認証が十分でなく不正ログインを受けたケース

クラウドサービスへログインする際に十分な認証がされておらず、不正ログインを受けてしまいました。
また、多要素認証を導入しているつもりが、以前から使用していた強度の低い認証方法を併用していたことで、そこから攻撃を受けてしまったケースも発生しています。



次ページで
POINTと対策例を解説します。

事例２　クラウドサービスへのログイン認証が十分でなく不正ログインを受けたケース

＜陥りやすいPOINT＞

- メールアドレスとパスワードだけの強度の低い認証方式を用いると簡単に推測されてしまう。
  また、複数のサービスでパスワードを使い回していると、他のサービスからパスワードが漏えいした場合に不正にログインされてしまうおそれがある。
- 多要素認証の一つとして携帯電話を利用する場合、携帯電話を持っていない従業員にはIDとパスワードのみでログインさせていたことにより、攻撃者に狙われることも考えられる。

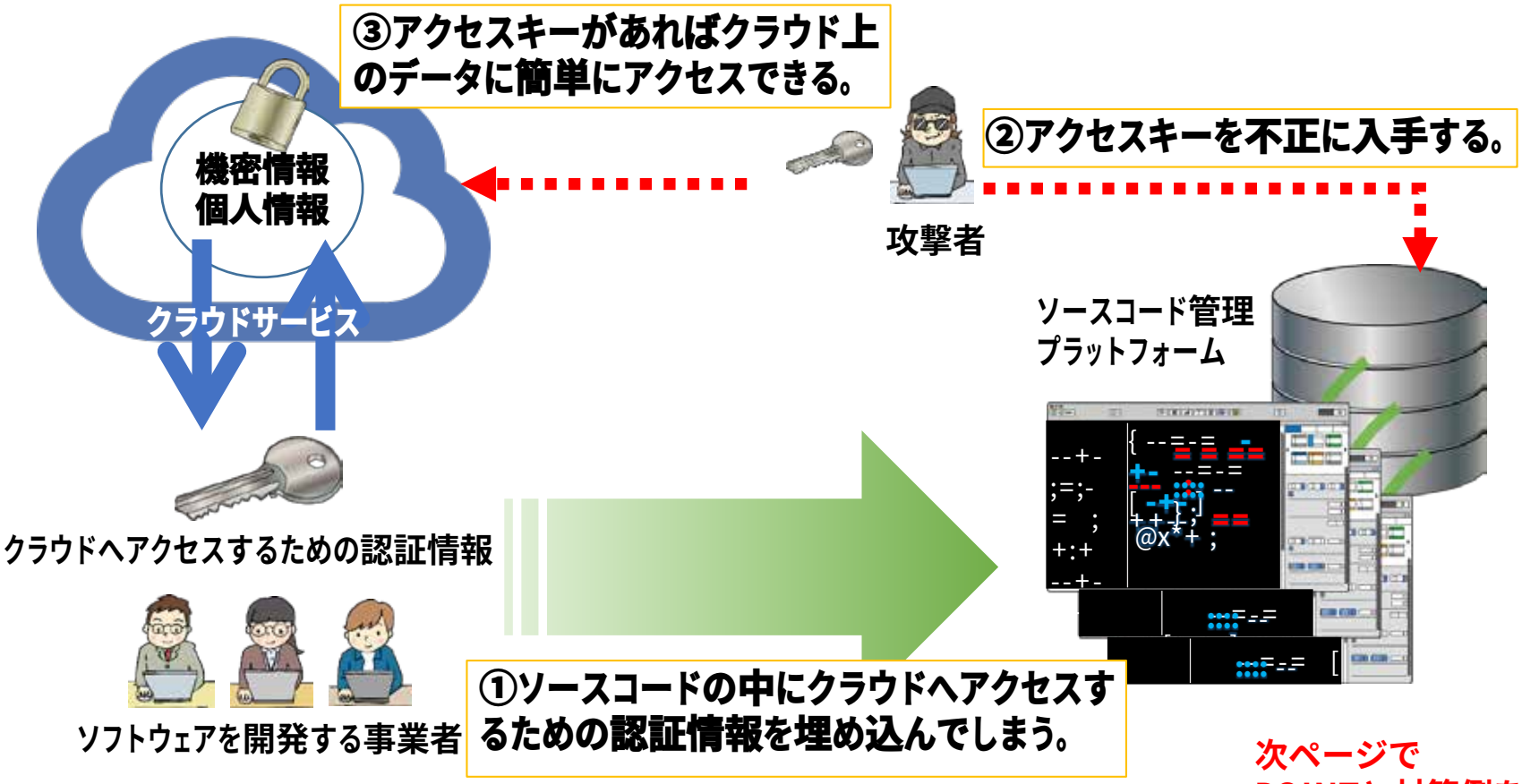
＜対策例＞

- パスワード等の認証情報が攻撃者に知られた場合に不正ログインされないよう、多要素認証を導入する。
- 携帯電話を持っておらず多要素認証ができない従業員のために例外的に用意した方法も含めて、セキュリティ対策として十分であるかを確認した上で認証方式を採用することが大変重要である。

Ø **多要素認証を導入した「つもり」とならないよう、従業員に提供している全てのログイン認証の方式が安全性が高い方式か確認してください。**

事例３　クラウドサービスのシステム管理者用の認証情報が適切に管理されていなかったケース

インターネット上のソースコード管理サービスを利用したところ、ソースコードの中にクラウドサービスのシステム管理者権限のIDやパスワードといった認証情報が含まれており、それらの認証情報を不正に入手した攻撃者からクラウドサービス上の個人情報等の機密情報に不正アクセスを受けてしまいました。



次ページで
POINTと対策例を解説します。

事例３　クラウドサービスのシステム管理者用の認証情報が適切に管理されていなかったケース

＜陥りやすいPOINT＞

- ソースコードにID/パスワードを直接記載してはいけない等のルールが徹底されておらず、ソースコードの中にクラウドサービスへの認証情報を埋め込んでしまっている。
- 複数の開発者で効率的に開発するためソースコードをインターネット上のソースコード管理サービスに公開している（公開範囲を限定していない）。
- クラウドサービスのシステム管理者アカウントのログイン認証に多要素認証を導入していない。

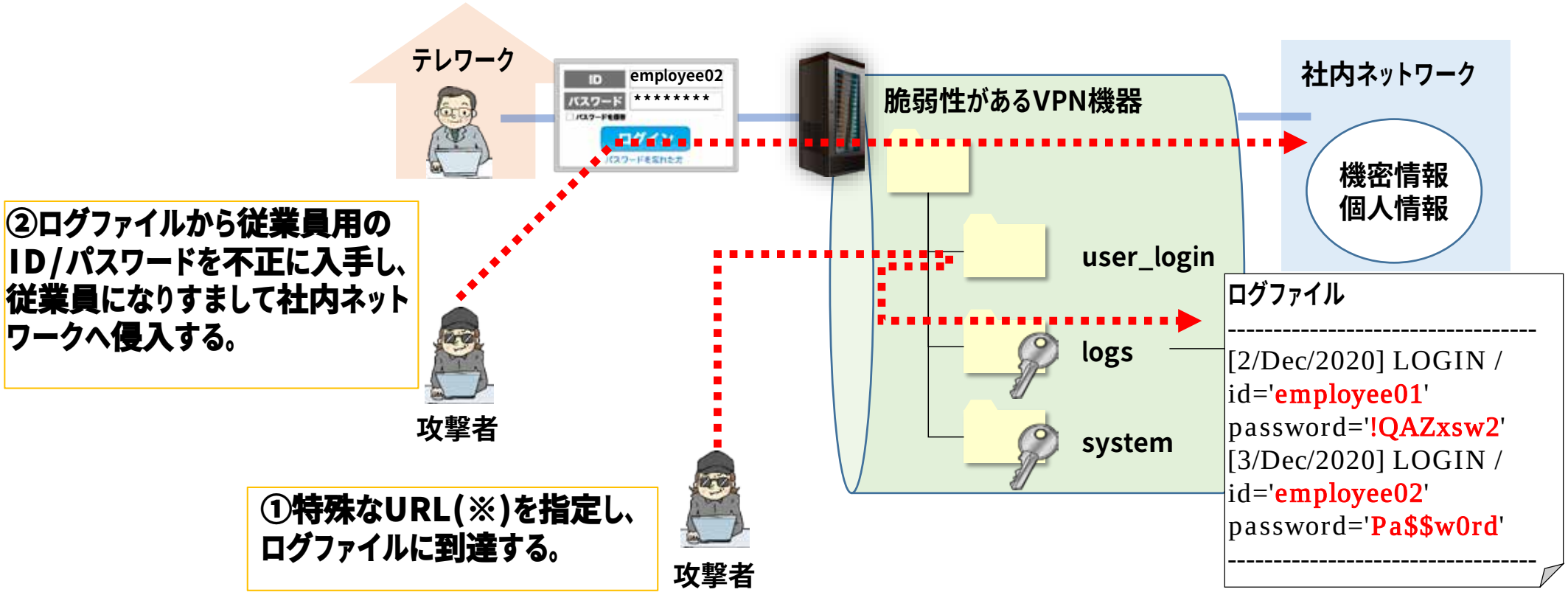
＜対策例＞

- ソースコードにID/パスワードやアクセスキー等の認証情報そのものを記載しない。
- インターネット上のソースコード管理サービスを利用する場合は、公開範囲を社内などに限定して利用する。
- クラウドサービスのシステム管理者アカウントのログイン認証に多要素認証を導入する。システム管理者アカウントの認証情報が漏えいするとクラウドサービスの全ての操作が行われてしまう危険性があるため、必要最小限の権限のアカウントを作成し利用する（万が一漏えいした場合の被害を最小限にする）。

- **クラウドサービスのシステム管理者権限の認証情報は、クラウドサービス事業者が推奨するベストプラクティス・管理ガイドラインに従い、第三者から見られることの無いよう安全な管理方法で保管してください。**

事例４　不正に入手したVPN認証情報を用いて個人情報を狙うサイバー攻撃

令和２年９月23日にテレワークに伴う個人情報漏えい事案について注意喚起を行っていますが、今もなお、テレワークで使用するVPN機器の脆弱性を突かれるサイバー攻撃による個人情報の漏えいが発生しています。



※「/../」などURLでは使わない文字列を記述する

次ページで
POINTと対策例を解説します。

事例４　不正に入手したVPN認証情報を用いて個人情報を狙うサイバー攻撃

＜陥りやすいPOINT＞

- VPN機器導入後、バージョンアップやセキュリティパッチの適用をしていない場合等、脆弱性の影響を受けるVPN機器をセキュリティ対策しないまま使用し続けると、攻撃者にVPN接続時のID/パスワードを窃取されるおそれがある。
- VPN接続時のID/パスワードを窃取されると社内ネットワークへ侵入されるおそれがあり、個人情報等の機密情報が窃取されたり、ランサムウェア（身代金要求型ウイルス）を用いた攻撃の被害を受けることがある。

Ø **VPN機器など職場外からのアクセスを目的とした機器の脆弱性を放置すると、大きな被害を受ける可能性が高いです。**

＜対策例＞

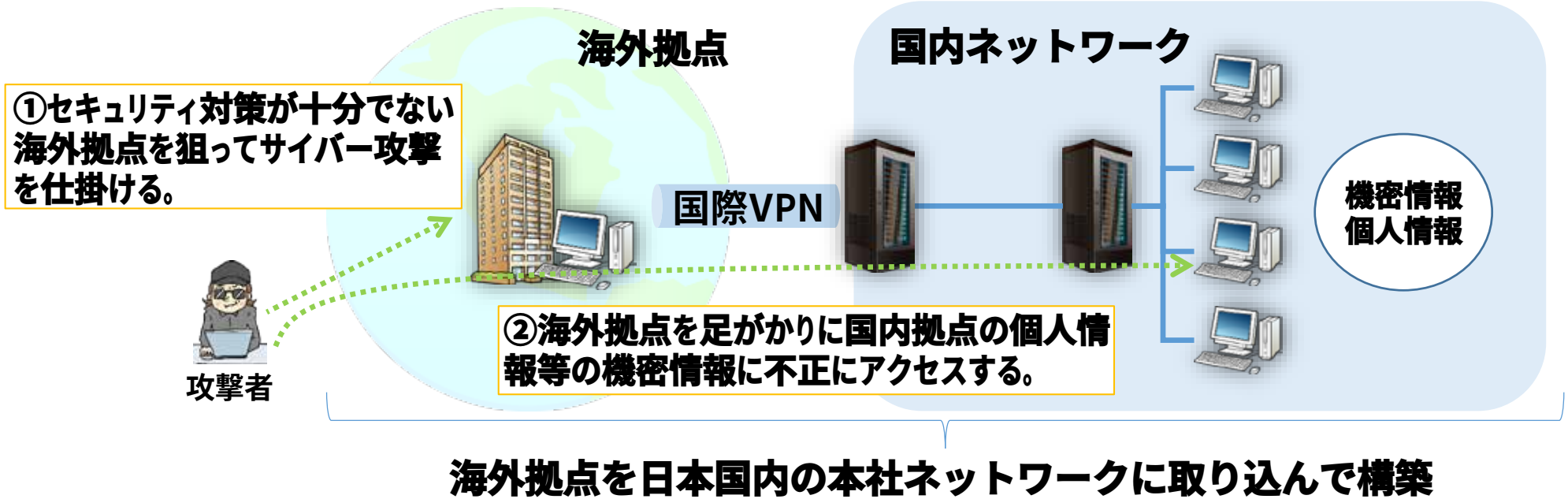
今一度、VPN機器のバージョンが最新であるか確認することを強くお願いします。最新のバージョンでない場合は、次に挙げるような対策や影響を軽減するための対応が必要です。

- 脆弱性の影響を受けないバージョンにアップデートする。
- VPN機器を経由するテレワーク等の認証に多要素認証を導入する。

Ø **脆弱性の影響を受けるバージョンを利用していた場合は既にID/パスワードが窃取されているおそれがあるため、アカウントのパスワードを変更することが望ましい。**

事例５ 海外拠点経由のサイバー攻撃により国内ネットワークまで侵入されたケース

ビジネスのグローバル化に伴って、海外現地支社、関連会社、取引先等の海外拠点を日本国内のネットワークに取り込んだ環境を構築したところ、日本国内に比べセキュリティ対策が十分でない海外拠点がサイバー攻撃を受けたことにより、国内ネットワークまで不正侵入され、個人情報等の機密情報にアクセスされてしまいました。



次ページで
POINTと対策例を解説します。

事例５ 海外拠点経由のサイバー攻撃により国内ネットワークまで侵入されたケース

＜陥りやすいPOINT＞

- 海外拠点は本社のガバナンスが行き届きにくく、システムの脆弱性への対策が十分でなかった。
- 海外拠点独自の運用により、管理されていない私用機器がシステムに接続されていた。
- コストが安価であることを優先し、セキュリティ対策が十分でないサプライチェーンを利用していた。

＜対策例＞

- 海外拠点であっても定期的にシステムの脆弱性情報を収集し、影響を受ける場合は迅速にバージョンアップする。
- 個人情報等の機密情報を保管するシステムを分離し、拠点間ネットワークのアクセス制限を強化する。
- サプライチェーンリスクの対策として、セキュリティ要件を定め、定期的にセキュリティ対策の実施状況を監査する。
- 万が一マルウェア感染等のサイバー攻撃を受けても早期に検知できるよう、振る舞い検知型のエンドポイントセキュリティ対策（EDR等）を導入する。

∅ **日本国内だけの対策で完結せず、海外拠点を含むネットワークをつないでいるグループ全体でセキュリティレベルを確保することが重要です。**

おわりに

　セキュリティ対策は、これだけ行えば十分というものがありません。世の中の脅威や情報セキュリティに関する事例を理解し、より一層適切なセキュリティ対策を講じ続けていく必要があります。

　個人情報保護委員会は、これまでにも個人情報取扱事業者向けに、個人情報を取り扱う上で発生しやすいヒヤリハット事例を紹介する「個人情報保護法ヒヤリハット事例集」、ECサイト等のウェブサイトを運営する事業者への注意喚起を個人情報保護委員会ウェブサイト上で公開しています。そちらも併せてご確認いただき、今後も必要なセキュリティ対策の検討・実施に役立ててください。

　確認いただく中で、個人データの漏えい等が確認された、もしくはそのおそれがある場合は、当委員会への報告をお願いいたします。